Nuclear Command, Control, and Communications (NC3) When Leaders Vanish: Bounded Pre-Delegation with Conflict-Aware Legitimacy Beacons and Decentralized Human Quorums

Douglas C. Youvan

doug@youvan.com

www.youvan.ai

October 23, 2025

The hardest NC3 problem isn't blast—it's absence. Imagine weeks of sophisticated spoofs and "pulled-back" probes, followed by a decapitation strike and leader flight: senior principals run to family or church, others freeze, Continuity of Government is fractured, and rival claims to authority emerge. Classic doctrines break differently. Fail-safe assumes present, decisive leaders; it stalls when none will decide. Fail-deadly assumes sensors and loss-of-command flags are trustworthy; in an adversarial deception campaign, it risks catastrophe. We propose bounded pre-delegation designed explicitly for leader absence or paralysis. Automation executes only reversible posture moves (disperse, alert, spin up airborne relays, open abort channels) when a multi-sensor quorum triggers. Weapons release still requires humans—but not named dignitaries. Instead, a minimal, geographically split human quorum is drawn from pre-certified role-based pools (duty officers, circuit judges, inspector-general delegates), validated by cryptographic legitimacy beacons that are *conflict-aware* (revocation, fork resolution, time-locks). We formalize quorum math when principals are missing, specify "anytime abort" dominance, design dark-start comms (VLF, airborne relays, protected SATCOM, troposcatter), and give procedures for contested or counterfeit authority. The aim is a constrained, auditable, governable NC3 that stays reversible and lawful when leaders are absent and ambiguity—not physics—is the main weapon.

Keywords:NC3, leader absence, paralysis, bounded pre-delegation, fail-safe, fail-deadly, deception, spoofing, conflicting legitimacy beacons, quorum math, role-not-name authorization, anytime abort, EMP, VLF, TACAMO, ALCS, dark-start communications, revocation, fork choice, governance, risk modeling.

A collaboration with GPT-5. 56 pages. CC4.0.

Outline

1. Threat Model: Ambiguity and Absence
   1.1 Weeks of spoofs, “pulled-back” probes, alert fatigue
   1.2 Decapitation strike → COG fragmentation
   1.3 Leaders flee or freeze: no uncontested chain of command
2. Failure Modes When No One Will Decide
   2.1 Physics & infrastructure: EMP, timing drift, satellite denial
   2.2 Human factors: fear paralysis, family-first exfil, moral injury
   2.3 Governance: constitutional succession vs operational reality in leader absence
3. Doctrine Triad Under Leader Absence
   3.1 Fail-safe: requires decisive principals → stalls without them
   3.2 Fail-deadly: fills the vacuum with automation → catastrophic FP risk under deception
   3.3 Bounded pre-delegation: reversible automation + decentralized human quorum
4. Decentralized Human Quorum, Role-Not-Name
   4.1 Pools not persons: duty officers, inspector-general delegates, circuit/judge pairs, allied liaisons
   4.2 Geo-split selection: algorithmic draw ensuring geographic and institutional diversity
   4.3 Minimal quorum sizes: 2-of-N or 3-of-M across separated regions and institutions
   4.4 Liveness guarantees: fallback expansion if some pools are unreachable
5. Legitimacy Beacons with Conflict Handling
   5.1 Beacon design: pre-committed key shards, time-locked attestations, tamper-evident custody
   5.2 Conflicting beacons: fork taxonomy (replay, captured keys, partitions, counterfeit issuers)
   5.3 Fork choice & revocation: epoch counters, shard-diversity thresholds, CRLs on low-bandwidth channels
   5.4 Beacon failure mode: automatic downgrade to posture-only state until conflict clears
6. Multi-Sensor Quorum & Adversarial Filtering
   6.1 Heterogeneous confirmation (space/ground/seismic/EM/radiation/OPINT)
   6.2 Independence weighting and veto rules; no single feed decisive
   6.3 AI as filter, not decider: red-teamed spoof resistance, uncertainty budgets
7. Anytime Abort Dominance
   7.1 More nodes authorized to abort than to execute
   7.2 Bandwidth priority for cancellation; short, redundancy-coded EAMs
   7.3 Immutable receipts; automatic rollback to safest prior state

8. Dark-Start Communications Under EMP/Denial
   8.1 Layered paths: VLF shore, airborne VLF (TACAMO), protected EHF SATCOM, troposcatter
   8.2 Health beacons to distinguish silence, jamming, capture
   8.3 Timing resilience: holdover clocks, anti-spoof time windows, crypto grace periods
9. Pre-Delegated Posture Moves (Reversible Only)
   9.1 Disperse forces, sortie comms relays, unlock abort channels, raise survivability
   9.2 No weapons release without decentralized quorum confirmation
   9.3 In-band drill labeling to prevent "boy-who-cried-wolf" erosion
10. Procedures When Principals Are Missing or Frozen
   10.1 Automated quorum summons: paging role-pools via all channels
   10.2 Substitution ladders: auto-promotion of alternates after bounded delays
   10.3 Counterfeit-order hygiene: reject orders lacking beacon + quorum proofs
   10.4 Safe timeouts: default to abort/stand-fast when conflicts persist
11. Risk Model with Leader Absence
   11.1 FP/FN definitions and cost weights (accidental launch vs failed response)
   11.2 Sensitivities: deception intensity, comms attrition, quorum unavailability
   11.3 Results: how decentralized quorums reduce FN without raising FP
12. Scenario Walkthrough
   12.1 Timeline: weeks of spoofs → decapitation → conflicting beacons → principal paralysis
   12.2 Behavior of Fail-safe vs Fail-deadly vs Bounded pre-delegation
   12.3 Decision points: when posture escalates, when quorums decide, when abort prevails
13. Governance, Law, and Ethics
   13.1 Mapping role-pools to constitutional succession and statutory authority
   13.2 Civil-military safeguards; allied witness attestations as tie-breakers
   13.3 Moral calculus with absent leaders; preserving reversibility under fear
14. Validation and Wargaming
   14.1 Red-team beacon forks, mass spoof drills, quorum-loss exercises
   14.2 Metrics: fork-resolution latency, quorum liveness, abort latency, posture reversibility
   14.3 Update cadence, key refresh, external assurance cells, rollback plans

15. Conclusion: Governable Power Without Present Principals
    15.1 Why decentralized human quorums + conflict-aware beacons are the least-bad path
    15.2 Near-term upgrades: pool certification, beacon rollout, drills
    15.3 A standard for auditable, reversible NC3 when leaders are absent or afraid

References

Appendices

1. Threat Model: Ambiguity and Absence

1.1 Weeks of spoofs, "pulled-back" probes, alert fatigue

- Adversary objective. Shift our priors from vigilance to complacency, then strike when our filters are lax.
- Tactics.
    - Multi-phenomenology spoofs: falsified flash/radiation/seismic cues; replayed telemetry; lookalike EAM formats with near-valid counters.
    - Identity deepfakes: cloned voices/faces of principals; compromised social channels; forged press guidance.
    - Network fog: jamming and partial outages that resemble mundane failures (weather, solar, maintenance).
    - Pulled-back probes: limited kinetic/cyber actions that halt just before clear thresholds, training operators to expect stand-downs.
- Effects.
    - Baseline drift: thresholds quietly ratcheted upward; alarms reclassified as nuisance.
    - Cognitive depletion: watch teams normalize deviation; escalation becomes socially costly.
    - Metric rot: on-time false alarms dominate dashboards; true-positive sensitivity falls.
- Indicators to log. Rising cancel rate after near-threshold alerts; growing counterfeits detected at the edge; widening gap between sensor-triggered and human-escalated events.

1.2 Decapitation strike -> COG fragmentation

- Event. A concentrated strike disables or isolates top decision nodes; national Continuity of Government (COG) plans activate under degraded comms.
- Immediate fractures.
    - Geographic partitions: regions lose synchronization; independent cells claim continuity.

    - Legal vs operational split: constitutional succession exists on paper; operational custody of keys and circuits does not match it.
    - Beacon forks: multiple cryptographic legitimacy beacons circulate (stolen shards, replays, unsynchronized epochs).
- Practical consequences.
    - Order collision: mutually exclusive execute/abort messages, each bearing some validity proofs.
    - CRL lag: revocations and key-burn notices propagate slowly on low-bandwidth survivable links.
    - Ambiguous time: GPS loss and stratum drift muddy counters, windows, and freshness checks.
- Design requirement. Default the system to posture-only (reversible moves) under beacon conflict until fork-choice rules confirm a single, lawful quorum.

1.3 Leaders flee or freeze: no uncontested chain of command

- Observed behaviors.
    - Flight to family/faith spaces and physical non-availability.
    - Moral shock/paralysis in remaining principals; refusal to sign irreversible orders.
    - Competing claimants emerge (some authentic, some counterfeit).
- System response we require.
    - Role-not-name authorization: draw decision authority from pre-certified role pools (duty officers, inspector-general delegates, circuit/judge pairs), not specific dignitaries.
    - Geo-split minimal quorum: 2-of-N or 3-of-M across separated regions and institutions; liveness timers auto-expand the pool if unreachable.
    - Anytime abort dominance: more nodes may send a valid abort than an execute; abort has bandwidth priority and shortest message formats.
    - Conflict-aware legitimacy beacons: epoch counters, shard-diversity thresholds, and revocation proofs; on unresolved conflicts, system locks to reversible posture.

    - Operator hygiene: reject orders lacking both (a) quorum proofs and (b) beacon conformity; treat charisma, titles, and media presence as non-factors.

- Outcome we aim for. A governable NC3 that can act reversibly without named principals, hold fire under contested authority, and still converge on a lawful human decision once a conflict-resolved quorum is live.

2. Failure Modes When No One Will Decide

2.1 Physics & infrastructure: EMP, timing drift, satellite denial

- EMP and ionospheric disturbance. High-altitude bursts scramble HF skywave, raise noise floors, and create regional "radio blackouts." VLF remains usable but slow; expect message truncation pressure and queuing delays that distort tempo-based procedures.
- Power and clock fragility. Loss of grid, GNSS jamming/spoofing, and holdover clock drift corrupt time-bounded cryptography (nonces, counters, freshness windows). Result: orders fail validation, or—worse—replays pass because windows are mis-estimated.
- Link-layer diversity collapses unevenly. EHF SATCOM suffers scintillation and pointing constraints; HF is chaotic; commercial backhauls are untrusted; LOS/troposcatter are range-limited; airborne relays need sortie time and protected basing. Asymmetry invites order races (who reaches whom first sets the de facto truth).
- Key-material reachability. Physical custody chains (vaults, couriers, authenticator kits) break on road closures, base lockdowns, or contaminated zones. Split custody fails "closed" if even one leg is missing.
- Telemetry ambiguity. "Silence" is indistinguishable among outage, jamming, capture, or self-imposed EMCON without health beacons and link-quality metadata. In a vacuum, humans overfit: either freeze or overreact.

2.2 Human factors: fear paralysis, family-first exfil, moral injury

- Acute threat appraisal failure. Weeks of spoofs degrade trust; then real signals arrive. Operators face contradictory priors ("probably fake" vs "this time is real"), producing choice paralysis and timeouts.
- Attachment and duty conflict. Some principals leave posts to secure family or faith communities. Others remain but avoid irreversible choices to avert personal culpability; risk-shifting replaces decision-making.

- Cascading moral injury. Conflicting execute/abort orders, uncertainty about lawful authority, and high-casualty stakes produce moral distress that further suppresses initiative. Informal “shadow vetoes” emerge (quiet noncompliance, foot-dragging).
- Cognitive load saturation. Alarm floods, degraded UX, and poor triage make it impossible to distinguish signal from noise. Without decision scaffolds (timers, checklists, contradiction-highlighting), staff either lock up or latch onto the first seemingly coherent narrative (which may be counterfeit).
- Social dynamics under stress. Rank inversion (a resolute junior, a hesitant senior), rumor cascades, and performative compliance (“copying orders” without executing) create a misleading appearance of control.

2.3 Governance: constitutional succession vs operational reality in leader absence

- Paper chain vs live chain. Statutory succession presumes reachable, consenting principals. After decapitation and dispersal, the operational chain is whoever can speak on authenticated channels with custody of means. These sets may not overlap.
- Conflicting legitimacy beacons. Captured keys, replayed attestations, unsynchronized epochs, and regional partitions produce beacon forks. With no fork-choice rule, forces face dueling “lawful” commands.
- Judicial and legislative latency. Courts and legislatures cannot convene at speed or securely. Ex post ratification is moot if irreversible actions occur first. Governance must embed ex ante rules for contested authority.
- Allied and interagency friction. Allies may possess corroborating evidence and readiness posture, but policy mismatches (nuclear sharing, ROE, national caveats) complicate alignment. Mixed messages worsen domestic ambiguity.
- COG activation gaps. Relocation sites, alternates, and liaisons may be stocked for continuity but not for conflict resolution under deception. Without role-not-name quorums and revocation/CRL channels, COG becomes a message repeater, not a legitimacy resolver.

Implication. In the moment when no one will decide, failure is not singular but interlocking: physics distorts channels, clocks corrupt trust primitives, humans freeze or flee, and governance lacks a live method to arbitrate legitimacy. The architecture must therefore assume absence, bound automation to reversible moves, and instantiate decentralized, conflict-aware quorums that can lawfully act when named principals cannot.

3. Doctrine Triad Under Leader Absence

3.1 Fail-safe: requires decisive principals → stalls without them

- Core idea. Weapons release requires explicit authorization from identified, senior officials along a statutory chain (names, not roles).
- Strengths (in normal times). Very low accidental-launch (FP) risk; strong civil control; clean accountability.
- Brittleness under absence.
    - Liveness failure: if principals are missing, fragmented, or morally unwilling, lawful orders never materialize; timeouts accumulate until opportunities (including aborts) expire.
    - Comms coupling: degraded links plus identity-bound authorization create a single point of failure: *this* person, *on this* circuit, *in this* window.
    - Deception leverage: sophisticated spoofs shift priors toward "another fake," encouraging *do nothing* even when signals are real.
- Observed pathologies. "Shadow vetoes" (quiet non-execution), performative compliance (ack without action), and escalation aversion ("no one wants to be *the* signer").
- Net effect. Conditional on attack, false negatives (FN) dominate: the system preserves legitimacy by defaulting to inaction, even when decisive (reversible) posture moves would reduce harm.

3.2 Fail-deadly: fills the vacuum with automation → catastrophic FP risk under deception

- Core idea. Pre-arm an automated backstop; if multi-sensor evidence + loss-of-command criteria are met, a machine pathway triggers retaliation without human assent.
- Strengths (on paper). Guarantees a response under decapitation; restores deterrence credibility if leaders or links are destroyed.
- Failure channels in adversarial ambiguity.
    - Sensor gaming: prolonged spoof campaigns raise the probability of a quorum of convincing—but false—indicators (replay, counter manipulation, timing skew).
    - Command-loss mimicry: jamming/partitions can counterfeit "lost leadership," satisfying the second precondition.

    - Pre-arming exposure: the very act of arming raises the base rate of catastrophic outcomes to "tiny but non-zero" across long crises.

- Governance deficit. No human legitimacy check at the decisive step; post-hoc oversight is meaningless after an irreversible act.
- Net effect. False positives (FP) become the dominant existential risk in the exact environment the adversary is shaping: *contested truth + broken comms + missing leaders*.

3.3 Bounded pre-delegation: reversible automation + decentralized human quorum

- Core idea. Split the problem.
    1. Automation may execute reversible posture moves (disperse forces, raise alerts, sortie airborne relays, open abort channels) when a multi-sensor quorum crosses predefined thresholds.
    2. Weapons release still requires a minimal, geographically split human quorum, drawn from role-based pools (duty officers, inspector-general delegates, circuit/judge pairs)—validated by conflict-aware legitimacy beacons (epoch counters, shard diversity, revocation proofs).
- Why it survives leader absence.
    - Role-not-name authorization: liveness without dignitary presence; quorum membership is algorithmically drawn from pre-certified pools.
    - Anytime-abort dominance: more nodes can send a valid abort than execute; cancellation has priority bandwidth and the shortest formats.
    - Fork-aware legitimacy: when beacons conflict (captures, replays, partitions), the system locks to posture-only until fork-choice rules converge—eliminating irreversible moves under contested authority.
- Spoof-resilient mechanics.
    - Heterogeneous sensing: independent phenomenologies (seismic, EMP/EM, radiation, OPINT) weighted for independence; no single feed decisive.
    - Time discipline under denial: holdover clocks, windowed counters, monotonic epochs; CRLs and key-burns propagated on low-bandwidth survivable links.
    - Receipts, not vibes: every action emits an immutable audit record binding signals, quorums, and keys used.

- Risk posture (intuitive summary).
    - Compared to fail-safe, bounded pre-delegation reduces FN by allowing machines to buy time and posture the force while humans are assembled.
    - Compared to fail-deadly, it caps FP by forbidding automation from crossing irreversibility and by privileging abort under conflict.
- Doctrine in one line. *Automate what you can undo; require decentralized, conflict-verified humans for what you cannot.*

4. Decentralized Human Quorum, Role-Not-Name

4.1 Pools not persons: duty officers, inspector-general delegates, circuit/judge pairs, allied liaisons

- Principle. Authority attaches to roles that are pre-vetted and continuously staffed, not to named dignitaries who may be absent or compromised.
- Core pools (illustrative, adaptable by statute):
    - Duty officers (operational): rotating O-6/O-7 equivalents at strategic commands with current NC3 certifications.
    - Inspector-general delegates (integrity): standing representatives empowered to attest to legality and rule conformance.
    - Circuit/judge pairs (civil oversight): pre-cleared federal judges and alternates, briefed on NC3 thresholds and secrecy protocols.
    - Allied liaisons (witnesses): treaty or nuclear-sharing partners authorized to co-sign as witness only, never sole execute.
- Eligibility baselines.
    - Active clearance; recent NC3 training; secure custody of authentication kits; acceptance of anytime abort doctrine.
    - Continuous performance telemetry (drills, response times, error rates) feeding a readiness score.
- Exposure control.
    - No pool member holds enough cryptographic material to act alone.

- Rotating duty and sealed-until-drawn selection to minimize targeting and coercion.

4.2 Geo-split selection: algorithmic draw ensuring geographic and institutional diversity

- Goal. A quorum that cannot be captured by one region, one service, or one building.
- Inputs.
  - Pool roster with attributes: region_id, service/branch, institution_type, readiness_score, comms_status.
  - Policy constraints: max_same_region = 1, max_same_institution = 1, min_diversity_score >= D.
- Selection sketch (sealed, auditable):

1. Compute eligible set E = { members with readiness >= R and comms_status == GREEN }.

2. Use a verifiable random function (VRF) seeded by a public beacon (e.g., timing epoch) to shuffle E.

3. Walk the list, adding candidates that keep diversity constraints satisfied until quorum size Q is met.

4. Emit a selection receipt: hash(E), seed, ordered picks, constraint proofs. Store on an append-only log.

- Denial resistance. If VRF seed channels are jammed, fall back to pre-shared deterministic seeds per epoch; adversary cannot predict the final set without full E and epoch state.

4.3 Minimal quorum sizes: 2-of-N or 3-of-M across separated regions and institutions

- Design rule. Favor the smallest quorum that still enforces diversity to minimize time-to-decision under attack.
- Typical profiles (examples, policy-tunable):
  - Execute path: 3-of-M where members span at least 3 distinct regions and 2 institution types (e.g., one duty officer, one IG delegate, one judge).
  - Abort path: 2-of-N with broader eligibility (more nodes may abort than execute) to enforce anytime abort dominance.
  - Witness path (allied): 1-of-K witness appended to execute records when available; never a gating requirement if unavailable.

- Constraint checks (machine-enforced before humans decide):
    - Distinct region_id and institution_type; freshness of credentials; beacon conformity (correct epoch, non-revoked shards); no conflict flags raised.
- Time windows. Short, explicit decision windows with auto-revalidation: if window W expires before Q signatures, selection refreshes and posture remains reversible.

4.4 Liveness guarantees: fallback expansion if some pools are unreachable

- Problem. Jamming, physical isolation, or casualty can starve the quorum.
- Liveness ladder (automatic, receipt-grade):
    1. T0: Attempt Q from primary pools under strict diversity constraints.
    2. T0 + t1: If short, expand geography (allow adjacent regions) while keeping institution diversity.
    3. T0 + t2: Broaden pools (e.g., alternate duty centers, retired-but-certified reserves on standby).
    4. T0 + t3: Reduce quorum size by one *only for abort*, never for execute.
    5. At all steps: System remains in posture-only (reversible moves) until execute quorum is met.
- Health beacons & timers. Each summoned member emits heartbeat + location-obscured liveness attestations. Non-responses trigger automatic substitution per the ladder.
- Fork containment. If conflicting legitimacy beacons appear at any stage, freeze execute, permit abort, and publish a fork ticket (epoch, signers, CRL state) to all comms legs.
- Auditability. Every selection, substitution, timeout, and vote produces a compact claim-check (hash chain, epoch, constraints satisfied) for after-action review and legal oversight.

Doctrine in practice. The quorum exists to bind irreversibility to humans without binding it to specific humans. Selection is cryptographically fair, diversity-constrained, denial-tolerant, and fast. When it cannot be met cleanly, the system does not guess: it stays reversible and privileges abort.

5. Legitimacy Beacons with Conflict Handling

5.1 Beacon design: pre-committed key shards, time-locked attestations, tamper-evident custody

- Purpose. A legitimacy beacon attests that an order originates from a *lawful office*, not a particular person, and that the office is occupied per succession law. It binds who may authorize, when, and under what constraints.
- Keying model.
    - Role keys, not personal keys. Each office in the succession line holds a role key $\boldsymbol{K_{role}}$protected in an HSM. Personal keys may co-sign as witness, but never substitute for $\boldsymbol{K_{role}}$.
    - Threshold shards. $\boldsymbol{K_{role}}$is split via $\boldsymbol{t}$ / $\boldsymbol{n}$secret sharing across geo-split custodians (e.g., clerk of court, IG safe, duty center). No single custodian can act alone.
    - Shard diversity. Custodians belong to distinct institutions (executive, judicial, oversight) to resist single-institution capture.
- Attestation structure (compact).
    - Header: role_id, beacon_epoch, validity_window, constraints_hash.
    - Body: state digest (e.g., current CRL root, succession table version, quorum ruleset id).
    - Signatures: threshold signature over header+body using $\boldsymbol{t}$ / $\boldsymbol{n}$shards; optional witness signatures (allied liaison, auditor) add context, not authority.
- Time discipline.
    - Time-locked attestations. Beacons carry monotonic epoch counters and bounded validity windows (e.g., 10 minutes) anchored to authenticated time sources with holdover rules under GNSS loss.
    - Grace windows. Small, asymmetric windows accommodate one-way links (VLF) and propagation asymmetries without enabling replays.
- Custody & tamper evidence.
    - HSM-only use. Shards never appear in clear; all signing occurs within sealed HSMs with rate limits and policy checks (cannot sign execute without quorum proof).

    - Custody logs. Movements of shards emit signed custody beacons (hash chains) broadcast over all channels; absence is visible systemwide.

- Distribution channels.
    - Multi-path broadcast: VLF shore, airborne VLF, protected EHF SATCOM, troposcatter, and store-and-forward buoys. Each packet carries link metadata for provenance triangulation.

5.2 Conflicting beacons: fork taxonomy (replay, captured keys, partitions, counterfeit issuers)

- Replay fork. A past-valid beacon is reintroduced after expiry to counterfeit current authority. Signal: valid signature, stale epoch, or expired window.
- Captured-keys fork. Adversary obtains a subset of shards and assembles a threshold using non-diverse custodians (e.g., multiple shards from one building). Signal: signatures verify, but diversity policy fails.
- Partition fork. Regions lose sync and emit divergent epochs or parallel succession tables (e.g., different acting officers). Signal: both beacons fresh and diverse, but state digests differ.
- Counterfeit-issuer fork. An unauthorized HSM or rogue CA enrolls a lookalike role_id. Signal: chain-of-trust breaks at root of authority; authentic CRL does not recognize the issuer.
- Timing-skew fork. Severe clock drift causes window overlaps and ambiguous freshness. Signal: inconsistent verified time sources across receivers; high variance in arrival times.

5.3 Fork choice & revocation: epoch counters, shard-diversity thresholds, CRLs on low-bandwidth channels

- Fork-choice rule (deterministic, auditable).
    1. Sanity screen. Reject beacons failing basic checks: signature invalid, window expired, role_id unknown.
    2. Diversity test. Accept only if the threshold signature proves custodian diversity across required institutions and regions.
    3. Epoch precedence. Prefer higher beacon_epoch; if equal, prefer the beacon whose constraints_hash matches the latest known policy digest.
    4. Recency & provenance. Prefer beacons observed on multiple independent channels within expected skew; penalize single-channel exclusivity.

5. Conflict quarantine. If two beacons both pass steps (1)–(4) yet disagree (role or constraints), enter posture-only and open fork-resolution.

- Revocation and slashing.
    - CRL beacons. A compact Certificate Revocation List (role ids, shard ids, HSM serials) is broadcast continuously in delta form over lowest-bandwidth links (VLF). Each delta is signed by a higher-order oversight role key with its own diversity requirements.
    - Key-burn attestations. If a shard is compromised, a burn beacon permanently invalidates it; all future thresholds must exclude it. Burn beacons are short and highest-priority on all channels.
    - Automatic slashing. HSMs that sign out-of-policy (e.g., execute without quorum proof) add themselves to auto-CRL, which peers verify and relay.
- Low-bandwidth pragmatics.
    - Bloom-filter CRLs. CRL deltas carried as Bloom filters shrink size while enabling fast “is this signer revoked?” checks on VLF.
    - Monotonic counters. Every CRL delta increments crl_epoch; receivers discard out-of-order deltas and request catch-up via any higher-bandwidth leg available.

5.4 Beacon failure mode: automatic downgrade to posture-only state until conflict clears

- Trigger conditions. Any of:
    - Multiple beacons for the same role pass cryptographic checks but conflict on constraints/state.
    - Diversity proof fails or cannot be verified due to missing metadata.
    - Time uncertainty exceeds the maximum skew budget for freshness tests.
    - CRL state is indeterminate (deltas missing or contradictory).
- Immediate system actions (machine-enforced).
    - Freeze irreversible paths. Block execute; continue or escalate reversible posture moves (disperse, alert, sortie relays, open abort channels).
    - Priority to abort. Accept abort commands from broader 2-of-N quorums; allocate bandwidth and retries preferentially to cancellation traffic.

    - Fork ticket issuance. Emit a compact fork ticket containing: observed beacon hashes, epochs, diversity proofs, CRL epochs, and channel provenance. Publish systemwide for human review and audit.
    - Summon decentralized quorum. Auto-page role pools in multiple regions to assemble the minimal human quorum empowered to adjudicate the fork per policy.
- Clearing the conflict.
    - Adjudication inputs: side-channel confirmations (physical custody checks), allied witness attestations, court escrow orders, and fresh CRL/burn beacons.
    - Convergence rule: proceed to execute-eligible state only when one beacon satisfies diversity, freshness, CRL consistency, and quorum ratification; otherwise remain posture-only.
- Audit & deterrence.
    - Every transition into and out of posture-only writes an immutable receipt (hash chain with epochs, rules applied, and quorums consulted). Publicly signaling this doctrine reduces adversary incentive to create beacon confusion, because it yields delay, not detonation.

Design ethos. Beacons are not a permission slip; they are a proof of lawful capacity bounded by time, diversity, and revocation logic. When proofs conflict, the system refuses irreversibility, privileges abort, and forces humans-in-quorum back into the loop.

6. Multi-Sensor Quorum & Adversarial Filtering

6.1 Heterogeneous confirmation (space/ground/seismic/EM/radiation/OPINT)

- Goal. Confirm (or falsify) attack indicators using independent phenomenologies so that a forged or degraded channel cannot tip the system.
- Sensor families (illustrative):
    - Space-based: nuclear burst detectors (optical/UV “double flash,” x/γ, EMP waveform tails), missile warning IR, GNSS integrity.
    - Ground/undersea: seismic arrays (yield/location estimation), hydroacoustic networks, infrasound.

    - EM spectrum: VLF noise spikes, HF blackout maps, wideband spectral occupancy, SATCOM anomalies, radar persistency.
    - Radiation/CBRN: fixed and mobile γ/β/α sensors, atmospheric samplers, neutron counters; dose-rate gradients over time.
    - Operational INT (OPINT): force movements, sortie rates, coded message tempos on known nets ("Pip," "Squeaky Wheel," allied equivalents), logistics telemetry.
- Cross-check patterns:
    - Causal chain coherence: (flash → overpressure → EMP → ionization → seismic/hydroacoustic) must align in time-of-arrival and geospatial dispersion within physics bounds.
    - Negative evidence: absence of expected second-order effects (e.g., no seismic where a high-yield surface burst is claimed) counts explicitly against the hypothesis.
- Data hygiene: each family produces (signal, time, location, quality, provenance) tuples with immutable hashes and link-layer metadata for later audit.

6.2 Independence weighting and veto rules; no single feed decisive

- Independence model.
    - Assign each feed $\boldsymbol{i}$a conditional independence score $\boldsymbol{I_i} \in [\mathbf{0}, \mathbf{1}]$reflecting hardware/vendor diversity, physical separability, and attack correlation.
    - Maintain a correlation matrix $\boldsymbol{C_{ij}}$(learned + red-team updated) capturing known couplings (e.g., shared power, common satellite bus, identical firmware).
- Weighted quorum test (sketch).
    - For an "attack present" hypothesis $\boldsymbol{H}$, accumulate evidence weight

$$\boldsymbol{W(H)} = \sum_{\boldsymbol{i \in S^+}} \boldsymbol{\alpha_i} \cdot \mathbf{log}\, \frac{\boldsymbol{P(s_i \mid H)}}{\boldsymbol{P(s_i \mid \neg H)}}$$

where $\boldsymbol{\alpha_i} = \boldsymbol{f(I_i, C_{i\setminus *})}$down-weights correlated feeds.

    - Require multi-family coverage: ∃at least k distinct phenomenology classes contributing $> \boldsymbol{\tau}$each (e.g., space + seismic + EM).

    - Negative veto: if any physics veto is triggered (e.g., seismic impossible for claimed yield/location), force posture-only regardless of $\boldsymbol{W}(\boldsymbol{H})$.

- No single feed decisive. By policy, no single class (e.g., space IR or social-media INT) can clear the execute gate. Even perfect-looking space data must be co-witnessed by at least one independent terrestrial phenomenology.
- Time windows & skew. Evidence must land inside a coherence window $\boldsymbol{\Delta t}(\boldsymbol{H})$derived from propagation physics; early/late arrivals are counted but penalized.
- Degradation transparency. Every decision computes and logs (coverage, independence, vetoes, skew) so humans see *why* the system did—or did not—advance.

6.3 AI as filter, not decider: red-teamed spoof resistance, uncertainty budgets

- Role boundary. AI filters and scores; humans-in-quorum decide. Models cannot directly authorize irreversible actions.
- Adversarially trained pipelines.
    - Red-team corpora: curated spoof sets (replayed flashes, GAN'd spectra, synthetic seismic, SATCOM mimicry, deepfaked voices).
    - Counterexample mining: continuously inject near-miss anomalies to harden decision margins; require models to output counterfactuals ("what would have to change for me to flip?").
- Model outputs (contract).
    - Likelihood ratios per feed with calibrated confidence intervals; no single "attack score."
    - Attribution tags: which features drove the score (e.g., "double-flash ratio," "Schumann resonance spike," "HF MUF collapse map").
    - Uncertainty budget: decomposition of error sources—sensor noise, time sync, missing channels, correlation penalties.
- Guardrails.
    - Immutable receipts: every inference stores model version, weights hash, training epoch, and input hashes; decisions are reproducible.
    - Two-man AI rule: any model update affecting thresholds requires dual approval from separate oversight pools; automatic rollback on anomaly spikes.

    - Fail-forward to reversibility: when uncertainty exceeds policy bounds, the AI can only recommend reversible posture moves and quorum summons, never execute.

- Human UX under overload.
    - Triage views: show coherence timelines (stacked by phenomenology), coverage heatmaps, and veto flags first; raw feeds available but not required.
    - Contradiction highlighting: surface the strongest disagreeing evidence and propose cheap adjudications (e.g., “task airborne VLF relay to region X” or “query allied seismic station Y”).
    - Timers & checklists: explicit countdowns to re-validate stale inputs; one-click “hold posture / broadcast abort” with pre-filled rationale templates.
- Metrics that matter.
    - False-positive/negative under red-team scenarios (per family and joint);
    - Fork-resolution latency (time to resolve conflicting sensors/beacons);
    - Abort latency (time from conflict detect → fleet-wide cancellation receipt);
    - Posture reversibility rate (fraction of escalations rolled back cleanly).

Bottom line. A multi-sensor quorum insists on diverse physics, explicit independence, and hard vetoes; AI sharpens signal from noise but cannot cross irreversibility. When evidence conflicts—or confidence falls—automation buys time with reversible posture, summons a decentralized human quorum, and privileges abort until the picture clears.

7. Anytime Abort Dominance

7.1 More nodes authorized to abort than to execute

- Asymmetric authority sets.
    - Execute quorum: small, diversity-constrained (e.g., 3-of-M spanning ≥3 regions and ≥2 institution types).
    - Abort quorum: broader (e.g., 2-of-N) with wider eligibility pools (additional duty centers, alternates, certified reserves, allied witnesses as non-gating co-signers).

- Why asymmetry matters. Execution is irreversible; cancellation is reversible and safety-preserving. The system therefore lowers the barrier for stopping motion relative to starting it.
- Machine enforcement. Radios/HSMs refuse to transmit or act on an execute without full execute-quorum proof, but will accept an abort from any 2-of-N set that passes freshness + revocation checks.
- Geographic liveness. At least one abort-eligible node exists in every theater and at sea (e.g., TACAMO aircraft, SSBN comms hubs), guaranteeing a nearby path to cancellation under partitions.
- Operator UX. “One-gesture abort”: authenticated consoles expose a single action to broadcast an abort with the minimum valid signature set; execution requires two-step confirmation with explicit constraint checks.

7.2 Bandwidth priority for cancellation; short, redundancy-coded EAMs

- Priority queues on all links. VLF, airborne VLF, EHF SATCOM, troposcatter, LOS: ABORT messages occupy the highest QoS class, preempting routine traffic and even execute confirmations.
- Compact format (illustrative 160–240 bits before coding).
    - Header (32–48b): msg_type=ABORT, link_id, phenom_bitmap, policy_version.
    - Epoch & counters (32–48b): beacon_epoch, crl_epoch, nonce.
    - Scope (16–24b): force_selector (e.g., all, region, leg, unit class).
    - Reason code (8–12b): fork_detected, time_uncertain, revocation_seen, human_veto, sensor_veto.
    - Auth (≥64b): threshold signature tag (2-of-N); truncated witness tags optional.
- Redundancy for bad channels.
    - Outer code: strong FEC (e.g., rate-1/3 convolutional or LDPC tuned per link).
    - Inner code: Raptor/ fountain style chunking so partial reception suffices to reconstruct.
    - Repetition: staggered bursts over multiple frequencies/legs with randomized interleaves to beat fading and jamming.

- Idempotence & dedupe. Each abort carries a monotonic abort_epoch; receivers apply first-seen valid abort ≥ current epoch and ignore duplicates/replays.
- Receiver behavior. On first valid ABORT:

1. Cease execute actions immediately;
2. Ack upstream with a micro-receipt (tiny "ACK-ABORT" burst);
3. Propagate downstream (store-and-forward) even if not tasked as a relay node.

- Testing cadence. Daily/weekly silent-to-operators line tests (checksum beacons) reserve capacity so that real aborts encounter known-good paths under load.

7.3 Immutable receipts; automatic rollback to safest prior state

- Receipts everywhere. Every node that sends, relays, receives, or enforces an abort emits a signed receipt containing: abort_epoch, local time hash, link provenance, action taken (e.g., "silo X safed," "airborne relay canceled"). Receipts are append-only and gossip-propagated across legs.
- State machine (irreversible lines guarded).
    - States: SAFE → POSTURE_UP → EXECUTE_ARMED → EXECUTE_ISSUED.
    - Abort transitions:
        - From any state, ABORT ⇒ roll back one or more steps to the nearest safe reversible state (e.g., EXECUTE_ARMED → POSTURE_UP; POSTURE_UP → SAFE).
        - Guards: If an irreversible boundary has been crossed (e.g., EXECUTE_ISSUED to a delivery platform that cannot be recalled), the system halts further escalation, logs last reversible point, and prioritizes damage-limiting procedures.
- Automatic rollback actions (examples).
    - Crypto: invalidate execute tokens, rotate nonces, advance abort_epoch to prevent stale executes.
    - Comms: tear down execute circuits, reallocate bandwidth to CRL/burn beacons and receipt aggregation.
    - Ops: stand down airborne relays not needed for safety; close launch enable lines; restore safing pins/permits; reverse posture flags in C2 displays.

- Fork-aware persistence. If aborts and executes collide in transit, nodes resolve by policy: ABORT supersedes unless the local ledger proves post-irreversible status; all collisions are flagged with conflict receipts for forensic review.
- Assurance & audit.
    - Merkle-chained logs: device-local and fleet-wide; periodic cross-signing by independent oversight keys.
    - Challenge audits: red-team injects synthetic aborts to verify preemption, latency, and dedupe; failures automatically quarantine offending nodes (relegated to receive-only).
    - KPIs: fleet-wide abort-to-enforcement latency (P50/P95), receipt coverage (% nodes acknowledging), rollback completeness (% posture elements reversed), collision rate (abort vs execute).

Operational doctrine in one line: *Make stopping easy and fast, make going hard and slow.* The architecture biases the system—cryptographically, procedurally, and at the PHY layer—so cancellation dominates execution under uncertainty, ensuring that when truth is contested, the default outcome is reversibility.

8. Dark-Start Communications Under EMP/Denial

8.1 Layered paths: VLF shore, airborne VLF (TACAMO), protected EHF SATCOM, troposcatter

- Design goal. Establish a dark-start comms posture—able to originate, authenticate, and propagate critical traffic with no prior synchronization, no grid, and severe spectrum denial.
- VLF shore (24–28 kHz class).
    - Role: Bedrock, one-way reach to submerged/remote forces; highest EMP tolerance; global/night-favored propagation.
    - Pros/cons: Extremely resilient; very low bitrate (tens to low hundreds of bps effective after FEC). Ideal for EAMs, CRL deltas, beacons, not bulk C2.
    - Dark-start tactic: Pre-reserved “lifeboat slots”—predictable micro-windows per hour for emergency traffic; guard bands dedicated to abort/C RL/burn beacons.

- Airborne VLF (TACAMO analog).
    - Role: Rapidly deployable VLF relay with trailing wire antennae, extending coverage and overcoming local ground-station loss.
    - Pros/cons: Mobile, survivable, can pattern orbits around blackout zones; constrained sortie basing and on-station endurance.
    - Dark-start tactic: “Sprint-to-grid” launch profile: first aircraft airborne within minutes to seed time/auth beacons, then form daisy-chained store-and-forward over denied regions.
- Protected EHF SATCOM (anti-jam LPI/LPD).
    - Role: Medium bandwidth for command backhaul, quorum coordination, receipts; nulls and spot beams mitigate jamming; crosslinks reduce ground reliance.
    - Pros/cons: Vulnerable to pointing, scintillation, or regional denial; requires terminal power and time sync.
    - Dark-start tactic: Blind-acquisition modes with widened search cones, coarse time from VLF, then converge to narrow-beam, high-assurance sessions.
- Troposcatter/LOS fallbacks.
    - Role: Regional, line-of-sight independent of ionosphere; rugged, trailer-deployable links across 50–300 km (tropo) or more (multi-hop).
    - Pros/cons: Terrain/weather dependent; lower throughput than SATCOM but far higher than VLF.
    - Dark-start tactic: Pre-surveyed aiming solutions and auto-beamforming profiles; carts wake into pre-shared frequencies with emissions control (EMCON) profiles.

Routing principle: Any-to-any, store-and-forward, multi-path. Messages are chunked (fountain-coded), tagged with provenance and epoch, and opportunistically ferried by whichever leg is live; ABORT and CRL/burn traffic preempts all queues.

8.2 Health beacons to distinguish silence, jamming, capture

- Problem. “No traffic” can mean: outage, jamming, enemy capture, EMCON, or compromised node. Treating all silence alike feeds bad decisions.
- Beacons (tiny, frequent, cryptographically signed).

    - Liveness beacon: “I am alive, at security level S, with keyset K, observing link health H” (≤128–256 bits before FEC).
    - Integrity beacon: “My HSM policy is intact; counters and CRL epoch = X; last command applied = Y.”
    - Custody beacon: For key shards/legitimacy beacons—“Shard in sealed custody at custodian class C; no sign events since T.”
- Channel heuristics to classify silence.
    - Outage: No RSSI floor, no beacon remnants across multiple orthogonal legs; neighboring nodes report the same null.
    - Jamming: High RSSI/no decode, spectral features (sweepers, noise carpets); beacons succeed on non-adjacent legs.
    - Capture/tamper: Unexpected speech patterns (non-policy transmissions), beacon timing skew beyond budget, or policy-violating signatures (e.g., execute signed without quorum proofs).
    - EMCON: Pre-declared quiet windows accompanied by low-rate hollow beacons (headers only) to prove controlled silence.
- Machine response.
    - Outage: Route around; summon airborne relays or troposcatter.
    - Jamming: Hop, null, lower duty cycle; switch to spread/low-probability-of-intercept waveforms.
    - Capture suspicion: Quarantine node (receive-only), publish capture alert, require out-of-band custody checks.
    - EMCON: Respect quiet; continue to accept ABORT/CRL on carve-outs.

Outcome: Operators and algorithms can tell why it’s quiet and choose reversible posture vs quarantine vs re-route appropriately.

8.3 Timing resilience: holdover clocks, anti-spoof time windows, crypto grace periods

- Holdover clocks.
    - Discipline: Each node carries high-stability oscillators (e.g., OCXO/Rb) with documented drift budgets; clocks are locally steered by any trusted time (GNSS, Loran-e, allied VLF time codes) when available.
    - Budgeting: Policies express max skew per link and function (e.g., ±2 s for SATCOM session start; ±30 s for VLF EAM freshness) to bound replay risk.
- Anti-spoof time windows.
    - Windowed counters: Every message carries (epoch, window_id, nonce); accept only if epoch monotonic and window_id matches the receiver's admissible set given current skew.
    - Diverse time sources: Weight time feeds by independence (space, terrestrial LF/VLF, inertial holdover). If sources disagree beyond policy, enter posture-only and cue time adjudication (e.g., summon airborne time beacon).
    - Time beacons from air. Airborne VLF relays periodically emit hashed time anchors (co-signed by oversight keys) that receivers use to pull clocks back inside admissible windows without trusting GNSS.
- Crypto grace periods (safe but forgiving).
    - Grace-once semantics: On first validation failure due to marginal skew, attempt grace verification with expanded but capped windows, logging the exception.
    - Asymmetric grace: ABORT/CRL/burn get wider grace than execute—cancellation should succeed even in worse timing conditions.
    - Counter ratchets: Successful grace verifies advance local counters/epochs to prevent backsliding replays; failures trigger quarantine and operator summons.
- Receipts and re-validation.
    - All time corrections, grace uses, and counter ratchets produce signed receipts; periodic cross-sign checks make widespread time spoofing visible.

Net effect: Even with GNSS denied and spectrum chaotic, the system can speak sparingly, know the difference between silence modes, and keep cryptographic time good enough to authenticate abort/CRL swiftly while refusing to authorize irreversible executes until clocks and beacons agree.

9. Pre-Delegated Posture Moves (Reversible Only)

9.1 Disperse forces, sortie comms relays, unlock abort channels, raise survivability

- Disperse forces (mobility without commitment).
    - Aviation: taxi-to-arm/de-arm areas; launch to pre-briefed dispersal fields; orbit on fuel-constrained racetracks that can be recalled within minutes.
    - Maritime: SSBN/SNN deployment to pre-assigned patrol boxes; surface groups shift to emissions-controlled lanes; no weapons system enters an irreversible enable state.
    - Ground: road-mobile assets move from garrisons to hardened hide sites; logistics wheels prepositioned; no warhead mating or PAL-code enablement.
    - Safeguards: movement orders carry auto-expiry timers; if not revalidated, units self-revert to prior locations/DEFCON.
- Sortie comms relays (talk more, shoot never).
    - Airborne VLF/EHF relays: scramble TACAMO-like aircraft to seed time/auth beacons and provide store-and-forward; sortie plans include immediate recall/retask hooks.
    - Tropo/LOS kits: deploy trailerized nodes to pre-surveyed aimpoints; power-on with EMCON profiles; any node can be quarantined remotely on suspicion.
    - Safeguards: relay sorties are non-binding; fuel, crew duty, and basing constraints are tracked so they can be stood down cleanly.
- Unlock abort channels (cancellation first-class).
    - Widened authority: activate additional 2-of-N abort signers across regions; cache low-bit-rate abort tokens on forward nodes.
    - Bandwidth reservation: carve out highest-QoS lanes on VLF/EHF/tropo for ABORT/CRL/burn traffic; throttle nonessential chatter.
    - Safeguards: unlocks are time-boxed; lapsed unlocks auto-close unless extended by quorum.
- Raise survivability (reversible hardening).
    - Physical: shelter-in-place, electromagnetic shielding to non-destructive levels; hatch to hot but PAL “safe”; isolate nonessential loads.

- Cyber: elevate logging, enable write-protect states, rotate session keys; no irreversible crypto burns unless quorum-approved.
- People: rotate watch sections, push decision scaffolds (checklists/timers), move families to prearranged safe points to reduce desertion pressure.
- Safeguards: every posture change has a paired rollback (who, how, how fast) and a timer that forces revalidation or auto-revert.

9.2 No weapons release without decentralized quorum confirmation

- Bright line. Automation can posture the force but cannot cross the irreversibility boundary (arming, PAL enable, execute-to-shooter) without a minimal, geo-split human quorum.
- Machine checks before humans sign:
  - Beacon conformity: current legitimacy beacon passes diversity + freshness + CRL tests.
  - Sensor quorum: multi-phenomenology evidence meets independence thresholds; no physics veto active.
  - Time hygiene: local skew within policy; grace consumed only for abort, not execute.
  - Conflict-free state: no open fork ticket on authority or sensors.
- Human quorum semantics (examples).
  - Execute: 3-of-M across ≥3 regions and ≥2 institutions (e.g., duty officer + IG delegate + judge).
  - Abort: 2-of-N (broader pools) can supersede at any time, including mid-coordination.
- Non-bypassable controls.
  - PALs, enable lines, and execution circuits require a cryptographic “go capsule” that only the human quorum can assemble; automation cannot synthesize it.
  - HSM policy: refuse to sign execute artifacts without attached quorum proofs and rule hashes; log every denial.

- Deadlock behavior. If quorum cannot be reached (leaders absent, pools unreachable), the system remains in posture-only and continues to expand abort authority and summon alternates—it does not degrade into automated execute.

9.3 In-band drill labeling to prevent “boy-who-cried-wolf” erosion

- Positive identification of drills.
    - All exercise traffic carries a mandatory DRILL flag in the header, plus an exercise epoch and scenario id signed by a separate Training Authority key that cannot sign execute.
    - Shadow realism: payloads may mimic real formats, but DRILL headers are unforgeable; nodes treat unlabeled traffic as real by default.
- Operator UX designed for trust, not drama.
    - Displays show distinctive drill livery and a “drill provenance card” (issuing authority, scenario, bounds).
    - Critical actions in a drill still require real-world steps (e.g., posture escalations), but irreversible lines remain locked; receipts are logged to validate muscle memory.
- Guardrails against misuse.
    - Rate-limits & windows: hard caps on concurrent drills; blackout periods during real-world tension.
    - Geofencing: prohibit drill traffic in regions under active alerts or fork tickets.
    - Audit hooks: every DRILL flag and Training Authority signature is receipt-logged; any attempt to inject a drill flag into real traffic triggers automatic quarantine and investigation beacons.
- Anti-erosion cadence.
    - Short, purposeful drills that exercise specific paths (e.g., ABORT preemption) rather than full-spectrum theatrics; never degrade live system performance for training spectacle.
    - Post-drill hygiene: automatic reset receipts, key sanity checks, and baseline restoration (bandwidth, priorities, alerts cleared).

- Public doctrine signal. Adversaries learn that trying to hide real attacks in “exercise noise” is futile—real traffic lacks the DRILL authority signature and will force posture-only or abort unless a proper human quorum confirms.

Bottom line: Pre-delegated posture moves let the system buy time and survivability without locking into catastrophe. The architecture treats reversibility as a hard requirement, ring-fencing anything irreversible behind decentralized, conflict-aware human judgment—and it keeps trust healthy by clearly marking drills so operators don’t learn the wrong lesson.

10. Procedures When Principals Are Missing or Frozen

10.1 Automated quorum summons: paging role-pools via all channels

- Trigger conditions (any):
    1. No valid execute response from named principals within T_exec_silence;
    2. Beacon conflict detected (fork ticket issued);
    3. Leader non-availability flagged (no liveness/health beacons from principal nets for T_leader_gap).
- Summons packet (≤ 320–512 b pre-FEC):
    - summons_type (execute_quorum | abort_quorum | adjudicate_fork)
    - epoch, window_id, nonce
    - role_pool_mask (duty, IG, judge, allied_witness)
    - diversity_constraints_hash (regions, institutions)
    - meet_vector (primary: EHF; fallback: VLF slot, troposcatter node, LOS grid)
    - proof_request (beacon epoch, CRL epoch)
    - auth (system HSM + oversight co-sig)
- Fan-out: VLF shore + airborne VLF + EHF SATCOM + troposcatter; store-and-forward by any node that receives.
- Receiver actions:
    1. Verify packet; 2) Emit liveness ACK (tiny signed receipt + link provenance); 3) Join ad-hoc quorum session on first viable leg; 4) Advertise constraints satisfied (region_id, institution_type) to the selector.

- Operator UX: A single “Summon quorum” control shows who is live, diversity coverage, time remaining, and missing constraints; red highlights for forks/time skew.

10.2 Substitution ladders: auto-promotion of alternates after bounded delays

- Goal: Ensure quorum liveness even with casualties, isolation, or fear paralysis.
- Ladder (policy-tunable):
    - Tier 0 (T0): Primary pools under full diversity constraints (e.g., Duty_O, IG_Del, Judge).
    - Tier 1 (T0+Δ1): Allow adjacent regions while preserving institution diversity.
    - Tier 2 (T0+Δ2): Admit alternates (e.g., certified reserve officers, magistrate judges).
    - Tier 3 (T0+Δ3): Reduce execute quorum size only if authorized by statute (rare); never below 3 and never relax diversity; abort quorum may drop to 2-of-N earlier.
- Promotion mechanics:
    - VRF-based selection (verifiable random function) using epoch-seed; publishes selection receipts (hash(E), seed, constraint proofs).
    - Non-responders auto-replaced; “two-strike” rule quarantines repeatedly unresponsive members for the current epoch.
- Bounded delays: Δ1/Δ2/Δ3 are short, explicit, e.g., 3/7/12 minutes for execute; half for abort. Timeboxes appear in all consoles; expired boxes force automatic tier advance.
- Safety rails: If at any tier beacon conflict or time uncertainty exceeds budget, promotion halts; system stays posture-only, expands abort authority, and escalates summons to broader pools.

10.3 Counterfeit-order hygiene: reject orders lacking beacon + quorum proofs

- Acceptance checklist (machine-enforced before an operator ever sees “execute”):
    1. Legitimacy beacon verifies: valid signatures, diverse shard proof, fresh epoch, CRL conformity;
    2. Quorum proof verifies: 3-of-M execute signatures spanning required regions/institutions; proof object includes role ids, time anchors, selection receipts;

3. Sensor quorum: independence threshold met, no physics veto;
4. Time hygiene: local skew within policy; no grace used for execute path;
5. No open fork ticket for the same role/epoch;
6. Message provenance: observed on ≥2 orthogonal legs (e.g., EHF + VLF) within skew budget.

- Fail-closed behavior:
  - Missing any element ⇒ hard reject; emit rejection receipt with reason codes (beacon_stale, diversity_fail, fork_open, time_uncertain, single_leg).
  - Suspicious but not disqualifying ⇒ quarantine to posture-only and page adjudication quorum.
- Operator hygiene: UIs hide "execute" actions until a complete proof bundle passes; abort remains one-gesture with minimal proof (2-of-N).
- Content hygiene: Strip identity-based cues (names, voices, seals) from decision panes; only proof objects and physics evidence are presented.

10.4 Safe timeouts: default to abort/stand-fast when conflicts persist

- Why: In ambiguity, the greatest risk comes from irreversible error; doctrine must make doing nothing lethal less likely than doing the wrong irreversible thing.
- Timeout taxonomy:
  - Quorum timeout: quorum not assembled by T_quorum_max ⇒ remain posture-only; refresh summons at higher tier; expand abort authority.
  - Beacon timeout: fork not resolved by T_fork_max ⇒ freeze execute path; require fresh beacon epochs or revocation/burn beacons; periodically re-poll custody out-of-band.
  - Sensor timeout: evidence fails to cohere by T_sensor_max ⇒ drop evidence weight, re-baseline, and stand-fast while continuing reversible posture.
  - Time-sync timeout: skew > budget for T_time_max ⇒ accept ABORT/CRL with widened grace; refuse EXECUTE.
- Automatic actions at timeout:
  - Broadcast ABORT-READY posture (unlock abort channels, reserve bandwidth, keep relays aloft);

- Issue status beacons summarizing which tests failed (quorum_liveness, beacon_conflict, sensor_incoherence, time_skew);
- Trigger adjudication scripts (e.g., physical custody checks, allied witness polls) and schedule next review window.

- Receipts & accountability: Every timeout emits a signed timeout receipt with inputs/thresholds at failure. Post-event audits can reconstruct why the system held fire.
- Human message (doctrine): *When legitimacy, physics, or time disagree, we do nothing irreversible.* The machine buys time with reversible posture, summons more humans, prefers abort, and documents every choice for later review.

11. Risk Model with Leader Absence

11.1 FP/FN definitions and cost weights (accidental launch vs failed response)

- Event space. Let $\boldsymbol{A} \in \{\mathbf{0}, \mathbf{1}\}$denote a real adversary attack during a crisis window; $\mathbf{Pr}\,(\boldsymbol{A} = \mathbf{1}) = \boldsymbol{p}$.
- System decision. $\boldsymbol{D} \in$ {EXECUTE,POSTURE-ONLY,ABORT}. For loss accounting, collapse to $\boldsymbol{L} \in \{\mathbf{0}, \mathbf{1}\}$where $\boldsymbol{L} = \mathbf{1}$implies irreversible force employment occurred.
- Outcomes.
  - False Positive (FP): $\boldsymbol{A} = \mathbf{0}$and $\boldsymbol{L} = \mathbf{1}$(accidental launch). Probability $\boldsymbol{P_{fp}}$.
  - False Negative (FN): $\boldsymbol{A} = \mathbf{1}$and $\boldsymbol{L} = \mathbf{0}$(failed response). Probability $\boldsymbol{P_{fn}}$.
- Costs. Assign catastrophe-weighted losses: $\boldsymbol{C_{fp}} \gg \boldsymbol{C_{fn}} > \mathbf{0}$. Expected loss per crisis window:

$$\mathbb{E}[\text{Loss}] = \boldsymbol{P_{fp}}\,\boldsymbol{C_{fp}} + \boldsymbol{P_{fn}}\,\boldsymbol{C_{fn}}.$$

We report both the decomposed probabilities and the costed sum to show trade-offs.

- Driver variables (conceptual):
  - Evidence sufficiency $\boldsymbol{E}$from multi-sensor quorum (with independence penalties).
  - Comms integrity $\boldsymbol{K}$(probability decisive orders can propagate/return receipts).
  - Human availability $\boldsymbol{H}$(probability a valid execute-quorum can assemble on time).
  - Deception load $\boldsymbol{S}$(probability spoof sets pass pre-filters).

- Pre-arming fraction $\boldsymbol{q}$(share of time any fail-deadly backstop is armed).

11.2 Sensitivities: deception intensity, comms attrition, quorum unavailability

We express $\boldsymbol{P_{fp}}$and $\boldsymbol{P_{fn}}$for the three doctrines as functions of $(\boldsymbol{S}, \boldsymbol{K}, \boldsymbol{H}, \boldsymbol{q})$. Illustrative forms (policy-tunable):

- Fail-safe (FS).

$$\boldsymbol{P_{fp}^{FS}} \approx \boldsymbol{\epsilon}\text{(human blunder term, very small)}$$
$$\boldsymbol{P_{fn}^{FS}} \approx \boldsymbol{p} \cdot (\boldsymbol{1} - \boldsymbol{K} \cdot \boldsymbol{H})$$

Insight: Any hit to comms ($\boldsymbol{K} \downarrow$) or leader availability ($\boldsymbol{H} \downarrow$) linearly inflates FN.

- Fail-deadly (FD).

$$\boldsymbol{P_{fp}^{FD}} \approx (\boldsymbol{1} - \boldsymbol{p}) \cdot \boldsymbol{q} \cdot \boldsymbol{S^{\backslash *}} \cdot \boldsymbol{L_c}$$

where $\boldsymbol{S^{\backslash *}}$is the post-filter spoof success after independence/veto checks, and $\boldsymbol{L_c}$is the probability that command-loss mimics are present (jamming/partitions).

$$\boldsymbol{P_{fn}^{FD}} \approx \boldsymbol{p} \cdot [(\boldsymbol{1} - \boldsymbol{q}) \cdot (\boldsymbol{1} - \boldsymbol{K} \cdot \boldsymbol{H})]$$

Insight: Arming backstop ($\boldsymbol{q} \uparrow$) cuts FN when attack occurs, but multiplies FP with spoofable environments ($\boldsymbol{S^{\backslash *}} \uparrow$, $\boldsymbol{L_c} \uparrow$).

- Bounded pre-delegation (BPD).
  - Automation is capped at reversible posture, so FP arises only via human quorum:

$$P_{fp}^{BPD} \approx (1 - p) \cdot \pi_{ex} \cdot \delta$$

where $\pi_{ex}$is the probability an execute-quorum forms in a no-attack window, and $\delta$the chance that proofs + humans err simultaneously (tiny; often $\ll \epsilon$).

  - FN reflects failure to both posture adequately and form a quorum under attack:

$$P_{fn}^{BPD} \approx p \cdot [(1 - K_{post}) + (K_{post}) \cdot (1 - H_{dec})]$$

where $K_{post}$is the probability the posture stage ameliorates comms (airborne relays, alternate links) and summons, and $H_{dec}$the probability a decentralized quorum assembles (role-not-name) within time.

Sensitivity levers.

- Deception intensity S: Raises $S^{\setminus *}$for FD; BPD dampens via hard vetoes and locks at posture-only under conflict.
- Comms attrition K: Hurts FS most; BPD improves effective $K_{post}$by launching relays and reserving abort lanes.
- Quorum unavailability H: FS depends on named principals; BPD substitutes role pools, increasing H_{dec}.

11.3 Results: how decentralized quorums reduce FN without raising FP

- Directional result 1 (FN). With leaders absent/paralyzed ($H \downarrow$), FS FN approaches p. BPD reduces FN because posture automation raises $K_{post}$and decentralized pools raise H_{dec}. FD also lowers FN if pre-armed ($q \uparrow$), but at an FP cost.
- Directional result 2 (FP). Under high deception ($S^{\setminus *} \uparrow$) and comms partitions ($L_c \uparrow$), FD accumulates non-trivial FP even if numerically small per minute—large over long crises. BPD keeps FP near the human-error floor because automation cannot cross irreversibility, and abort dominance prefers cancellation under conflict.
- Directional result 3 (costed loss). For any $C_{fp} \gg C_{fn}$, the expected loss is dominated by FP in FD and by FN in FS; BPD typically minimizes the costed sum by shifting probability mass away from both extremes.

Illustrative numbers (one crisis window, not predictive):
Let $p = 0.01$, $K = 0.4$(heavy attrition), $H = 0.5$(leaders often absent), $S^{\setminus *} = 10^{-4}$, $L_c = 0.2$, $q = 0.2$. Then:

- FS: $P_{fp} \approx 10^{-5}$; $P_{fn} \approx 0.01 \cdot (1 - 0.4 \cdot 0.5) = 0.008$.
- FD: $P_{fp} \approx 0.99 \cdot 0.2 \cdot 10^{-4} \cdot 0.2 \approx 3.96 \times 10^{-6}$;; $P_{fn} \approx 0.01 \cdot (1 - 0.2) \cdot (1 - 0.4 \cdot 0.5) = 0.0064$.
- BPD (assume $K_{post} = 0.7$, $H_{dec} = 0.7$, $\pi_{ex}\delta \sim 10^{-8}$): $P_{fp} \approx 10^{-8}$;; $P_{fn} \approx 0.01 \cdot [(1 - 0.7) + 0.7(1 - 0.7)] = 0.0039$.

Takeaway. In leader-absence scenarios, decentralized quorums plus reversible posture automation cut FN roughly in half relative to fail-safe—without paying fail-deadly's FP price. The

doctrine choice then becomes explicit: if you value governability + reversibility under deception and broken comms, BPD dominates the risk surface.

12. Scenario Walkthrough

12.1 Timeline: weeks of spoofs → decapitation → conflicting beacons → principal paralysis

Phase 0 — Shaping weeks (T–21 to T–1 days):

- *Spoofs & probes:* forged "double-flash" packets, replayed seismic, deepfaked press hits; minor cyber/kinetic probes that stop short.
- *Operator effect:* thresholds creep upward; alarms reclassified as nuisance; watch teams expect stand-downs.
- *System posture (ours):* low-rate health/legitimacy beacons running; drills carry explicit DRILL headers; ABORT lanes quietly tested.

Phase 1 — Strike (T0):

- *Event:* coordinated decapitation—DC/alt sites struck; regional jamming; GNSS spoofing; partial grid failure.
- *Sensors:* space-based flash/EMP tails; patchy seismic; HF blackout maps; VLF still viable.
- *Comms:* SATCOM degraded; VLF shore stations alive; TACAMO launchable.

Phase 2 — Beacon conflict (T0+10–40 min):

- *Fork:* two role beacons appear—both fresh; one fails shard-diversity; CRL deltas lag on VLF.
- *Orders:* contradictory "execute/stand-fast" packets circulate, each with some proofs.
- *Clocks:* skew widening; grace used for ABORT only.

Phase 3 — Principal paralysis (T0+40–120 min):

- *Human picture:* named principals unreachable; some flee; others refuse irreversibles.
- *Operational picture:* regions partition; rumors of capture; allied liaisons online.

Phase 4 — Stabilization (T0+2–6 h):

- *Quorum summons:* role-based pools paged; geo-split 3-of-M execute quorum partially formed; 2-of-N ABORT quorum fully live.

- *Fork resolution:* revocation/burn beacons arrive; custody checks clear one beacon; clocks re-disciplined by airborne time anchors.
- *Outcome:* either (a) lawful execute quorum confirms; or (b) posture-only persists with periodic re-adjudication; ABORT remains dominant.

12.2 Behavior of Fail-safe vs Fail-deadly vs Bounded pre-delegation

Phase	Fail-safe (FS)	Fail-deadly (FD)	Bounded pre-delegation (BPD)
0 — Shaping	Ignores many alerts; doctrine intact.	May pre-arm if leadership authorizes; FP risk starts accumulating over time.	Quietly tests ABORT lanes, validates beacons, refreshes role pools; drills clearly labeled.
1 — Strike	Waits for named principals on degraded links; liveness failure likely.	If pre-armed and criteria met (sensors + loss-of-command), auto-retaliation path primes; humans optional.	Auto-posture only: disperse, sortie relays, unlock ABORT channels, raise survivability; no irreversible steps.
2 — Beacon conflict	Deadlock—legal authority contested; no execute.	Knife-edge: spoofable sensors + partitions can satisfy triggers → FP pathway.	Hard lock to posture-only; fork ticket issued; ABORT has priority; summons decentralized quorum.
3 — Paralysis	Stalls; competing claims unresolved; FN risk grows.	Automation may fire on mixed evidence if armed; no human legitimacy check at the last step.	Role-not-name quorum forms from duty/IG/judge pools; allied witness optional; clocks/time fixed via air beacons.
4 — Stabilize	If principals surface, execute possible; otherwise missed response.	If not armed or sensors inconclusive, oscillates; if armed & spoofed, accidental launch possible.	Two outcomes: (a) quorum + cleared beacon ⇒ execute; (b) conflict persists ⇒ stay reversible; ABORT wins any collision.

Bottom lines:

- FS preserves legitimacy but often fails to act under absence → FN dominant.
- FD ensures action but can be gamed in deception/partitioned environments → FP tail risk.

- BPD buys time with reversible automation, then binds irreversibility to a decentralized, conflict-aware human quorum; ABORT always easier than EXECUTE.

12.3 Decision points: when posture escalates, when quorums decide, when abort prevails

DP-1: Auto-posture trigger (T0–T0+5 min)

- Inputs: multi-sensor quorum crosses reversible thresholds; no physics veto; beacon status irrelevant.
- Action (BPD): disperse forces, launch comms relays, unlock ABORT channels, elevate cyber shields.
- Not allowed: PAL enable, go-capsule creation, execute circuits.

DP-2: Fork detection (T0+10–20 min)

- Inputs: conflicting legitimacy beacons or missing CRL deltas; time skew > budget.
- Action (BPD): freeze execute, issue fork ticket fleet-wide; widen ABORT authority; summon adjudication quorum.
- Outcome: posture continues; execute path blocked until fork clears.

DP-3: Quorum liveness test (rolling, every 3–7 min)

- Inputs: liveness ACKs from role pools; diversity constraints satisfied?
- Action: If short, advance substitution ladder (adjacent regions → alternates); never relax diversity for execute; may relax abort to 2-of-N earlier.
- Outcome: either quorum forms (proceed to DP-4) or posture persists.

DP-4: Execute admissibility check (immediately on quorum)

- Machine checks: fresh beacon with shard-diversity; sensor independence threshold met; no physics veto; two-leg provenance; time within strict window.
- Human act: geo-split 3-of-M sign go capsule.
- Fail-closed: any check fails ⇒ stay posture-only; log rejection receipt.

DP-5: Abort collisions (any time)

- Condition: ABORT and EXECUTE messages cross in transit or arrive out of order.

- Policy: ABORT supersedes unless the receiver proves it has crossed an irreversible boundary; collisions produce conflict receipts; rollback to nearest safe state.

DP-6: Timeout governance (T0+X, repeating)

- Quorum timeout: quorum not formed ⇒ expand pools; keep posture reversible.
- Beacon timeout: no fork resolution ⇒ re-poll custody, require burn beacons; maintain posture-only.
- Sensor timeout: incoherent evidence ⇒ drop weight; refresh windows; maintain posture, avoid execute.
- Time-sync timeout: skew too large ⇒ widen grace only for ABORT/CRL; reject EXECUTE.

DP-7: De-escalation and receipts (post-event)

- If stand-down: auto-revert posture (pull relays, close abort unlocks), rotate keys/counters, consolidate immutable receipts.
- If execute occurred: preserve full proof chain (beacons, quorums, sensors, timers) for legal oversight and allied review.

Operational invariant: *Automate what you can undo; require decentralized, conflict-verified humans for what you cannot; and in any ambiguity, ABORT beats EXECUTE*.

13. Governance, Law, and Ethics

13.1 Mapping role-pools to constitutional succession and statutory authority

- Role-not-name, but still lawful. The role pools (duty officers, inspector-general delegates, circuit/judge pairs) are not substitutes for elected principals; they are temporary custodians of process empowered to *validate* or *withhold* irreversibility when the constitutional chain is nonfunctional. Their remit is codified in statute: they may authorize posture and co-sign legitimacy, but they cannot originate policy or expand use-of-force authorities.
- Binding to succession law.
    - Succession tables → Beacon policy. The legal line of succession is compiled into the legitimacy beacon constraints (role IDs, precedence, incapacitation tests) and versioned. Any change in law or appointment rolls updates the beacon constraints_hash.

    - Role pools as liveness bridges. If no successor can be contacted with valid proofs within bounded times, the system stays reversible; role pools can attest to the absence and convene adjudication, but cannot “become” the successor.

- Statutory authorities and fences.
    - Explicit grants: pre-delegations to posture (disperse, sortie relays, unlock abort channels) and to adjudicate conflict (fork-choice, CRL/burn issuance under oversight keys).
    - Explicit prohibitions: no authority to arm PALs, generate go-capsules, or alter Rules of Engagement.
    - Sunset & review: pre-delegations expire without periodic legislative reauthorization; after-action audits feed a statutory lessons-learned docket.
- Chain-of-custody to courts. Quorum selections, beacons, CRLs, and decisions generate immutable receipts admissible to a designated Article III panel for post-incident review—tying emergency conduct back to constitutional oversight.

13.2 Civil-military safeguards; allied witness attestations as tie-breakers

- Civilian primacy by construction.
    - Every execute quorum must include at least one civil-oversight role (e.g., judge/IG delegate); military-only quorums are structurally invalid.
    - Anytime-abort dominance gives civil nodes more opportunities to halt than to push—codified in HSM policies and link priorities.
- Dual-track oversight.
    - Operational chain (duty officers) and integrity chain (IG/judicial) co-sign all irreversible steps; either chain can veto progress back to posture-only.
    - Automated ethics checks: machine-enforced “guard clauses” (no execute under beacon conflict; no execute when time skew exceeds budget; no execute if physics veto fires).
- Allied witness attestations.
    - What they are: cryptographically signed witness beacons from designated allies (nuclear-sharing partners, treaty allies) affirming their independent sensor picture and governance status.

    - What they do: they do not confer authority to execute; they raise confidence in fork-resolution and reduce accidental divergence across coalitions.
    - When they matter: during partitioned comms or contested legitimacy, a quorum may require at least one allied witness to exit posture-only—unless time-critical, in which case witness beacons are logged post-hoc.
- Transparency without compromise. A public doctrine snippet (declassified essentials) signals: *irreversibility requires civil oversight + diversity; ambiguity yields delay, not detonation.* This reduces adversary incentive to manufacture confusion.

13.3 Moral calculus with absent leaders; preserving reversibility under fear

- Ethical centerline. When elected leaders are missing or frozen, the moral hazard is substituting technocracy for consent. Bounded pre-delegation avoids this by separating posture from employment: machines and role pools may buy time and survivability, but only a human, diversified quorum may cross the irreversible line—*and only when legitimacy is cryptographically and procedurally clear*.
- Asymmetry of harms.
    - False Positive (accidental launch) is ethically catastrophic, potentially civilization-ending; doctrine must make it extraordinarily hard.
    - False Negative (missed response) is also grave, but reversible posture (dispersal, shields, relays) mitigates harm while legitimacy is restored.
    - Therefore: bias for reversibility under uncertainty is the least-harm rule.
- Moral injury and agency. Operators facing dueling "authorities" need an ethics-backed right to refuse irreversibles without complete proofs—backed by policy (no retaliation for correct refusal), process (checklists, timers), and technology (UIs that hide execute without proofs). This preserves human dignity and moral agency when fear is high.
- Dignitary responsibility without presence. Absent leaders still bear ex post responsibility. Immutable receipts ensure a truthful ledger for legislative, judicial, and public scrutiny, preventing the quiet normalization of emergency shortcuts.
- Proportionality & last resort. Even when a lawful quorum forms, systems present least-harm options first (extended posture, targeted defensive actions) and require explicit justification to escalate beyond reversible measures.

- Aftercare and restitution. Post-crisis, the same receipts that constrained action enable transparent review, discipline for willful breach, and support for personnel who acted under duress—closing the ethical loop.

Governance credo: *Legitimacy before lethality; diversity before decisiveness; reversibility before resolve.* The architecture makes that credo operational, so that in the very moment when fear tempts shortcuts, the system itself keeps the country inside both law and ethics.

14. Validation and Wargaming

14.1 Red-team beacon forks, mass spoof drills, quorum-loss exercises

- Beacon-fork red teams (crypto/governance attack):
    - Objectives: Generate conflicting legitimacy beacons via replay, shard capture, counterfeit issuers, epoch skew, and regional partitions.
    - Methods:
        - Simulate stolen shard usage (non-diverse custodian sets) and verify diversity proofs catch it.
        - Inject replayed beacons with valid signatures but stale epochs; test CRL/Bloom-filter performance on VLF.
        - Emulate rogue issuer (fake CA/HSM serials) to test root-of-authority checks.
        - Force time desync across nodes to induce overlapping windows; confirm posture-only lock.
    - Success criteria: System auto-issues fork tickets, freezes execute, widens abort authority, summons adjudication quorums, and converges deterministically per fork-choice rules.
- Mass spoof drills (sensor/NC3 denial attack):
    - Objectives: Stress multi-sensor quorum and AI filters with coordinated false positives across space IR, seismic, HF blackout maps, and OPINT chatter.
    - Methods:
        - Replay near-real signatures (double-flash ratios, EMP waveforms, infrasound) with physics inconsistencies.

        - Jam/shape SATCOM and HF while leaving VLF paths intact; seed social deepfakes.
        - Measure AI's uncertainty budgets and hard physics vetoes under load.
    - Success criteria: Automation escalates posture-only; no irreversible gating; contradictions are surfaced; ABORT lanes remain dominant and low-latency.
- Quorum-loss exercises (liveness/governance attack):
    - Objectives: Prove decentralized, role-not-name quorums can assemble when principals are absent or frozen.
    - Methods:
        - Deny access to primary pools; degrade one region per epoch; simulate duty-center evacuation.
        - Exercise the substitution ladder (adjacent regions → alternates → reserves) and VRF-based selection receipts.
    - Success criteria: Execute quorum forms within bounded time *or* system stays posture-only while abort quorum remains live; all steps produce auditable receipts.
- End-to-end "decapitation + fog" campaign:
    - Combine forks + spoofs + quorum loss for multi-hour scenarios; observe fatigue effects; rotate blue teams to capture human factors.

14.2 Metrics: fork-resolution latency, quorum liveness, abort latency, posture reversibility

- Fork-resolution latency (FRL):
    - Definition: FRL $= t_{\text{clear}} - t_{\text{fork-ticket}}$.
    - Targets: P50 ≤ 12 min; P95 ≤ 30 min under mixed links.
    - Breakdown: time for CRL/burn propagation, custody checks, adjudication quorum assembly, and beacon re-issuance.
- Quorum liveness (QL):
    - Definition: Fraction of drills where a valid execute quorum forms within policy windows (T0→T_exec_max).

    - Targets: QL_exec ≥ 0.7 in stressed scenarios; QL_abort ≥ 0.95.
    - Sub-metrics: Diversity satisfaction rate (regions/institutions), substitution ladder depth used, VRF selection success without manual override.
- Abort latency (AL):
    - Definition: Time from ABORT issuance at origin → enforcement receipt at edge nodes.
    - Targets: P50 ≤ 90 s global; P95 ≤ 180 s with one major leg degraded.
    - Reliability: Receipt coverage (% nodes acknowledging within window) ≥ 0.98.
- Posture reversibility index (PRI):
    - Definition: Share of posture escalations that cleanly revert to SAFE within the planned rollback window.
    - Targets: PRI ≥ 0.97; Rollback completeness ≥ 0.99 for comms/cyber, ≥ 0.95 for logistics-heavy movements.
    - Collision rate: ABORT vs EXECUTE message collisions per 10k events; target → asymptotically zero with ABORT precedence correctly enforced.
- Time hygiene score (THS):
    - Definition: % decisions made with clocks within strict window; % grace used limited to ABORT/CRL.
    - Targets: THS ≥ 0.98 strict; Execute under grace = 0.
- Audit integrity (AIg):
    - Definition: % actions with valid, cross-signed Merkle receipts; log divergence events per 10k actions.
    - Targets: AIg ≥ 0.999; divergences autoremédiated < 60 s.

14.3 Update cadence, key refresh, external assurance cells, rollback plans

- Update cadence (doctrine + software):
    - Models & thresholds: Monthly minor updates; quarterly red-team recalibration; canary deployments to non-critical nodes first.

    - Doctrine & procedures: Semiannual review with legislature/oversight; after-action-driven amendments.
    - Freezes: Update blackout during elevated crises; only security hotfixes via pre-approved channels.
- Key refresh & shard hygiene:
    - Role keys: Rotate role-key shards on a 6–12 month cadence; diversify custodians on each cycle.
    - HSM policy updates: Signed by oversight keys with 2-of-2 approval (operational + integrity chain).
    - CRL discipline: Continuous delta broadcast on VLF; periodic full-state snapshots on EHF/tropo; burn beacons take absolute priority.
- External assurance cells (EACs):
    - Mandate: Independent teams (technical + legal + ethics) with compartmented access to logs and simulated environments.
    - Functions:
        - Run shadow wargames in parallel; compare blue decisions vs EAC counterfactuals.
        - Conduct supply-chain audits (firmware, time sources, HSM provenance).
        - Publish sealed findings to an Article III panel and select legislative overseers.
    - Rotation: Refresh membership annually; include allied observers under MOUs.
- Rollback plans (technical + doctrinal):
    - Software rollback: One-click version reversion baked into every node; immutable previous images stored offline; rollback receipts logged.
    - Policy rollback: Pre-signed policy snapshots (quorum sizes, veto rules) that can be reinstated by a minimal oversight quorum if a change degrades metrics.
    - Crisis rollback: If an update correlates with metric degradation (FRL↑, AL↑, PRI↓), auto-trigger rollback to last good within bounded time, broadcast rollback notice beacons, and quarantine new features.

- Continuous validation loop:
    - Plan → Drill → Measure → Adapt. Every exercise yields metric deltas; sub-targets create action items with owners and deadlines; unresolved deltas trigger focused re-drills within 30 days.
    - Transparency: Declassifiable metric summaries shared with stakeholders (and selectively with allies) to build deterrence by clarity: ambiguity will delay, not detonate.

End state: Validation is not a box-check—it is a standing campaign. Red teams attack authority and physics; metrics expose brittleness; updates are cautious and reversible; independent cells keep us honest. The result is an NC3 that stays governable, auditable, and reversible precisely when the world is least forgiving.

15. Conclusion: Governable Power Without Present Principals

15.1 Why decentralized human quorums + conflict-aware beacons are the least-bad path

When leaders are absent or paralyzed, the classical options both fail in predictable, opposite ways: fail-safe preserves legitimacy but risks paralysis (high FN), while fail-deadly guarantees action but can be gamed into catastrophe (tail-risk FP). Decentralized human quorums validated by conflict-aware legitimacy beacons carve a middle channel that is lawful, empirical, and survivable. They bind irreversible acts to diversified human consent—not to any single dignitary—and they make ambiguity self-limiting: beacon forks, time skew, or sensor contradictions can delay posture but cannot produce an automated launch. Coupled with a multi-sensor quorum and anytime-abort dominance, this architecture shifts probability mass away from both catastrophic error modes without pretending certainty is available in the fog. It operationalizes a simple ethic: *automate what you can undo; require plural, verified humans for what you cannot.*

15.2 Near-term upgrades: pool certification, beacon rollout, drills

- Pool certification (90–180 days). Stand up role-not-name rosters (duty officers, IG delegates, judge pairs, allied witnesses). Issue credentials, custody kits, and readiness telemetry. Legislate scope fences (posture yes; employment no).
- Beacon rollout (120–270 days). Deploy role-key shards in geo-split HSM custody; publish the initial constraints_hash (succession table, quorum rules). Stand up CRL/burn channels over VLF/EHF with Bloom-filter deltas.
- Drills (begin monthly, then quarterly full-spectrum).

    - Beacon-fork red teams: prove posture-only lock and fork resolution.
    - Mass-spoof campaigns: validate physics vetoes, independence weights, and AI uncertainty budgets.
    - Quorum-loss exercises: drive the substitution ladder and VRF selection receipts.
    - Abort sprints: repeatedly measure abort-to-enforcement latency and receipt coverage under denial.
- Doctrine & UI hardening. Hide “execute” paths without complete proof bundles; make one-gesture abort universal; publish a declassifiable doctrine snippet: *ambiguity yields delay, not detonation*.

15.3 A standard for auditable, reversible NC3 when leaders are absent or afraid

Set a measurable baseline that any NC3 design must meet in the age of deception and leader absence:

- Reversibility first. Irreversible boundaries (PAL enable, go-capsule issue) are cryptographically unreachable without a geo-split human quorum; ABORT always preempts and propagates faster than EXECUTE.
- Conflict aware by default. Beacon forks, time uncertainty, or sensor incoherence force posture-only; systems emit fork tickets and summon quorums automatically.
- Physics over narrative. Decisions cite multi-phenomenology evidence with independence weights and physics vetoes; identity cues are non-decisive.
- Receipts, not reassurances. Every action—summons, vote, beacon, CRL, abort, rollback—produces immutable, cross-signed receipts suitable for judicial and legislative audit.
- Cautious evolution. Updates ship with canaries, rollbacks, and external assurance cells; metrics (fork-resolution latency, quorum liveness, abort latency, posture reversibility) decide permanence.

This standard does not promise perfection; it promises governability. By engineering for diverse human consent, conflict-aware legitimacy, and reversible automation, we keep national power usable—and stoppable—when the usual guardians are missing, afraid, or under assault.

References

1. Congressional Research Service. Defense Primer: Nuclear Command, Control, and Communications (NC3), May 1, 2025. Congress.gov
2. Congressional Research Service. Nuclear Command, Control, and Communications (NC3) (In Focus IF11697), Aug. 15, 2025. Congress.gov
3. U.S. Navy. E-6B Mercury Airborne Command Post (TACAMO/ALCS) – Fact File, Sept. 22, 2021. Navy
4. NAVAIR. E-6B Mercury (program page), accessed 2025. Naval Air Systems Command
5. U.S. Space Force. Advanced Extremely High Frequency (AEHF) System – Fact Sheet, accessed 2025. U.S. Space Force
6. Director, Operational Test & Evaluation (DOT&E). AEHF Operational Assessment (FY2013), 2013. DOTE
7. U.S. Space Force. MILSTAR Satellite Communications System – Fact Sheet, accessed 2025. U.S. Space Force
8. National Academies. Appendix G: U.S. Satellite Nuclear Detonation Detection System (USNDS), in *Technical Issues Related to the Comprehensive Nuclear Test Ban Treaty*, 2012. National Academies Press
9. U.S. Air Force (AFTAC). Air Force Technical Applications Center – Mission Overview (USNDS/treaty monitoring), accessed 2025. 16af.af.mil
10. Peterson–Schriever SFB / USSF. AFTAC Detachment 46 – USNDS Sensors on GPS & DSP (fact sheet), accessed 2025. Peterson Schriever Space Force Base
11. National Museum of the U.S. Air Force. Emergency Rocket Communications System (ERCS) (fact sheet), accessed 2025. National Museum of the U.S. Air Force
12. Wikipedia. AN/DRC-8 Emergency Rocket Communications System (ERCS) (program history), updated 2025. Wikipedia
13. GlobalSecurity.org. Perimetr (“Dead Hand”) overview, Sept. 25, 2023. GlobalSecurity
14. Wikipedia. Dead Hand (Perimeter) (general background), accessed 2025. Wikipedia
15. Institute for Security and Technology. Effects of Electromagnetic Pulses on Communication Infrastructure (Report), Oct. 2024. Institute for Security and Technology

16. U.S. EMP Commission. Report of the Commission to Assess the Threat to the United States from EMP Attack – Executive Report, 2004. EMPCommission.org

17. U.S. Navy VLF. Jim Creek Naval Radio Station (NLK) – VLF site overview (HistoryLink), May 30, 2019. HistoryLink

18. Wikipedia. Jim Creek Naval Radio Station (NLK) (VLF 24.8 kHz, power), updated 2025. Wikipedia

19. Signal Identification Wiki. Jim Creek (NLK) (frequency/modulation notes), June 7, 2019. sigidwiki.com

20. George Washington University, National Security Archive. "Launch-on-Warning" Nuclear Strategy and Its Insider Critics, June 11, 2019. National Security Archive

21. *TIME* (Obituary). Stanislav Petrov… Feared History Repeating Itself, Sept. 2017. TIME

22. *The New Yorker*. World War Three, by Mistake (false-alarm history), Dec. 2016. The New Yorker

23. GAO. Nuclear Command, Control, and Communications: Update on DOD's Modernization Efforts (GAO-17-641R), Aug. 15, 2017. Government Accountability Office

24. GAO. Review of DOD's Current Modernization Efforts (GAO-14-414R), Mar. 18, 2014. Government Accountability Office

25. RAND Corporation. Modernizing the U.S. Nuclear Triad (Perspective PEA1434-1), 2022. RAND Corporation

26. Atlantic Council. Modernizing Space-Based NC3 (Issue Brief), July 15, 2024. Atlantic Council

27. DoD CIO. DoD C3 Modernization Strategy, 2021. (BLOS, SATCOM-denied comms), U.S. Department of Defense CIO

28. GAO. Defense Nuclear Enterprise: Systems Face Sustainment Challenges (GAO-20-296), Mar. 26, 2020. Government Accountability Office

29. Nautilus Institute (APLN). NC3 Country Profile / Synthesis Reports (Hayes et al.), 2019–2021. nautilus.org+1

30. U.S. Space Force, Space Systems Command. USNDS – Global near-real-time nuclear detonation detection (video description), accessed 2025. Space Systems Command

Notes: Items 12, 14, and 18 are used as aggregation points or for terminology; where possible, primary fact sheets (items 3–11, 15–16, 21, 27–28) anchor technical or doctrinal assertions.

Appendices

A. Formal quorum math and fork-choice pseudocode

A.1 Quorum feasibility and diversity constraints

Let $\mathcal{P}$be the set of eligible members, each member $u$labeled by:

- Region $r(u) \in \{1, \dots, R\}$
- Institution $i(u) \in \{$ops,oversight,judicial$\}$
- Readiness $w(u) \in [0,1]$
- Comms status $k(u) \in \{0,1\}$(1 = reachable)

A valid execute quorum $Q \subseteq \mathcal{P}$satisfies:

1. $| Q | \geq q_e$(e.g., $q_e = 3$)
2. $| \{r(u): u \in Q\} | \geq \rho$(e.g., $\rho = 3$)
3. $| \{i(u): u \in Q\} | \geq \iota$(e.g., $\iota = 2$)
4. $k(u) = 1$for all $u \in Q$
5. Optional: $\sum_{u \in Q} \quad w(u) \geq \tau$(readiness floor)

An abort quorum requires $| Q | \geq q_a$with $q_a < q_e$(e.g., $q_a = 2$), diversity relaxed but still requiring distinct regions OR institutions.

Feasibility test. Define binary variables $x_u \in \{0,1\}$and solve:

$$\min \sum_u \quad - w(u)x_u \text{s.t.} \sum_u \quad x_u \geq q_e, \ | \{r(u): x_u = 1\} | \geq \rho, \ | \{i(u): x_u = 1\} | \geq \iota, \ x_u \leq k(u)$$

(Use greedy + backtracking or VRF-seeded randomized rounding; feasibility, not optimality, is required under time bounds.)

A.2 VRF-seeded selection (receipt-grade)

Input: eligible set E, epoch ϵ, diversity constraints (ρ, ι)
Output: ordered candidate list π, selection receipt

seed ← VRF(GlobalBeacon || ε)

π ← Shuffle(E, seed)

Q ← ∅

for u in π:

  if Q ∪ {u} still satisfies diversity constraints (greedy test):

    Q ← Q ∪ {u}

    if |Q| = q_e: break

emit SelectionReceipt = Hash(E, ε, seed, order(π), chosen(Q), constraints)

If not enough, escalate substitution ladder (adjacent regions → alternates → reserves) and re-run.

A.3 Fork-choice pseudocode (conflict-aware beacons)

function ValidateBeacon(B):

  if !SigValid(B): return REJECT(sig_invalid)

  if B.epoch < Local.epoch: return REJECT(stale_epoch)

  if B.window_expired: return REJECT(expired_window)

  if !DiversityProof(B.shard_set): return REJECT(diversity_fail)

  if RevokedAny(B.shard_set, CRL): return REJECT(revoked_signer)

  return ACCEPT

function ForkChoice(B1, B2):

  v1 ← ValidateBeacon(B1); v2 ← ValidateBeacon(B2)

  if v1=REJECT and v2=ACCEPT: return CHOOSE(B2)

  if v2=REJECT and v1=ACCEPT: return CHOOSE(B1)

  if v1=REJECT and v2=REJECT: return POSTURE_ONLY, IssueForkTicket(B1,B2)

  # both ACCEPT but conflicting

  if B1.epoch > B2.epoch: prefer ← B1 else if B2.epoch > B1.epoch: prefer ← B2 else:

    if B1.constraints_hash = PolicyHash and B2≠: prefer ← B1

    else if B2.constraints_hash = PolicyHash and B1≠: prefer ← B2

else:

if MultiLegProvenance(B1) > MultiLegProvenance(B2): prefer ← B1

else if MultiLegProvenance(B2) > MultiLegProvenance(B1): prefer ← B2

else: return POSTURE_ONLY, IssueForkTicket(B1,B2)

return CHOOSE(prefer)

Any unresolved conflict ⇒ POSTURE_ONLY, widen abort authority, summon adjudication quorum, broadcast fork ticket.

B. EMP/ionospheric operational notes

B.1 Propagation regimes under nuclear EMP/ionization

- HF (3–30 MHz): Expect D/E-layer absorption spikes and MUF/LUF volatility; skywave blackouts regionally for minutes–hours. Treat HF as opportunistic only.
- VLF (3–30 kHz): Most resilient; supports ultra-low-bitrate, long-haul links. Reserve "lifeboat slots" for EAM/CRL/ABORT traffic. Plan for diurnal variation and path-specific fading; use repetition + strong FEC.
- EHF SATCOM (44 GHz class): Anti-jam/nulling helps, but scintillation and pointing jitter increase during geomagnetic disturbance; rely on blind-acquisition modes and broadened search windows at dark-start.
- Troposcatter (0.9–5 GHz): Independent of ionosphere; useful for regional backbones when SATCOM/HF are degraded; pre-surveyed aim points reduce setup time.

B.2 EMP hardening patterns

- Electronics: metalized gaskets, filtered penetrations, surge suppression, SEUs mitigated via ECC + watchdog resets; "safe default" on power loss.
- Cabling/antennas: choke/bonding at entry points, fiber where feasible; VLF antennas isolated via gas discharge + series inductors.
- Timing: OCXO/Rb holdover; disciplined to LF/VLF time beacons; bounded drift tables per function.

B.3 Procedures during blackout

- Message minimalism: prefer compact ABORT/CRL beacons; fountain-code chunking; staggered bursts across legs.
- Health beacons: maintain tiny signed liveness/integrity beacons to distinguish outage vs jamming vs capture.
- EMCON: codified quiet windows with hollow beacons; all exceptions logged.

C. EAM formats, counters, revocation and CRL sketches

C.1 EAM (Emergency Action Message) skeletons (illustrative)

- ABORT (highest priority; ~160–240 bits pre-FEC):
    - hdr (type=ABORT, policy_ver, link_id)
    - epoch (beacon_epoch, crl_epoch, window_id)
    - scope (force_selector)
    - reason (enum: fork_detected | time_uncertain | sensor_veto | human_veto)
    - auth (2-of-N threshold tag + optional witness tag)
- POSTURE (reversible move):
    - hdr (type=POSTURE, action_id)
    - epoch (as above)
    - ttl (auto-revert timer)
    - constraints (safety caps, e.g., “no PAL enable”)
    - auth (policy HSM + oversight co-sig)
- EXECUTE (gated by quorum; larger):
    - hdr (type=EXECUTE, op_id)
    - epoch (strict window; no grace allowed)
    - proof_bundle (legitimacy beacon digest, quorum proof 3-of-M, selection receipt, two-leg provenance attestations)
    - auth (go-capsule composite signature; PAL-gated)

C.2 Counters and freshness

- Monotonic epochs: beacon_epoch, crl_epoch, abort_epoch strictly increase; devices reject regressions.
- Windowing: window_id derived from admissible set given current skew; EXECUTE requires strict window match; ABORT accepts widened grace.
- Nonces: per-message nonces bound into signatures; dedupe caches handle repeats.

C.3 Revocation & CRL

- CRL delta (VLF-friendly):
    - crl_epoch (u32)
    - delta_bloom (k-bit Bloom filter of revoked IDs/HSM serials)
    - auth (oversight-role signature with diversity proof)
- Key-burn beacon (highest priority):
    - burn_id (shard/HSM id)
    - reason (compromise | policy_violation | capture_suspected)
    - auth (oversight + at least one judicial co-sig)
- Auto-slash: HSMs that sign out-of-policy self-report → peers propagate to CRL; quarantined until human review.

C.4 Receipts
All nodes emit Merkle-chained receipts for send/receive/enforce events:

receipt = H(prev_receipt || msg_hash || local_time || link_provenance || action_code)

sig = Sign(device_key, receipt)

Periodic cross-signing by oversight keys enables later verification.

D. Checklists for contested-authority ops and rapid re-validation timers

D.1 Contested-authority (fork) checklist

1. Detect & declare: Issue fork ticket with hashes/epochs of conflicting beacons.
2. Freeze irreversibles: Block EXECUTE paths; maintain/raise POSTURE.

3. Widen ABORT: Activate expanded 2-of-N authority; reserve bandwidth on all legs.
4. Summon adjudication quorum: Page role pools (duty, IG, judicial) with diversity constraints; start T_{quorum} timer.
5. CRL/Key-burn sweep: Request latest CRL deltas; poll for burn beacons; verify against Bloom filters.
6. Custody checks: Out-of-band challenges to shard custodians; log responses.
7. Time discipline: Compare time sources; if skew > budget, request airborne time beacons; no EXECUTE under grace.
8. Decide: If a single beacon passes diversity+freshness+CRL and quorum ratifies → EXECUTE eligible. Else remain POSTURE-ONLY.
9. Document: Log all steps with receipts; disseminate fork resolution status.

D.2 Rapid re-validation timers (examples, policy-tunable)

- T_posture_revalidate: 5–10 min. If not revalidated, auto-revert posture steps (pull relays, stand-down dispersal).
- T_CRL_poll: 2–3 min. Force CRL delta re-check; widen ABORT grace if CRL stale.
- T_time_resync: 4–6 min. If skew growing, request time beacons; suspend EXECUTE admissibility.
- T_quorum: 7–12 min tiers for execute; 3–6 min tiers for abort; triggers substitution ladder on expiry.
- T_fork_status: 10–15 min. Re-issue fork ticket summary + current adjudication status.

D.3 Counterfeit-order hygiene checklist

- Beacon signature valid? Yes/No
- Shard diversity satisfied? Yes/No
- Epoch/window fresh? Yes/No
- CRL epoch up-to-date and no revoked signer? Yes/No
- Two orthogonal comms legs observed (within skew)? Yes/No
- Sensor quorum met; no physics veto? Yes/No
- If any No → REJECT/POSTURE-ONLY, emit rejection receipt, summon quorum.

D.4 ABORT dominance checklist

- ABORT QoS lanes active on VLF/EHF/tropo? Yes
- Abort-eligible pools unlocked (2-of-N)? Yes
- Abort epoch incremented and distributed? Yes
- Edge nodes acknowledging ABORT within P95 target? ≥ target
- Any collisions (ABORT vs EXECUTE)? Investigate, ensure ABORT precedence enforced, log conflict receipts.

D.5 Post-event hygiene

- Consolidate receipts; run fork-resolution audit; rotate keys/counters; restore baselines (bandwidth, alerts); publish lessons learned and schedule targeted re-drills within 30 days.

Appendix ethos: tight math, deterministic rules, short messages, and visible receipts—so that under denial, deception, and absent leaders, the system stays lawful, auditable, and reversible.